ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МАТЕМАТИЧЕСКИЕ МЕТОДЫ

УДК 004.49

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКАХ: ВЗГЛЯД ИЗНУТРИ И СО СТОРОНЫ

***А.С. Бабурчик**, 1 курс*
*Научный руководитель – **И.А. Янковский**, к.э.н., доцент*
Полесский государственный университет

В IT–инфраструктуру крупного банка, как правило, входят до нескольких сот информационных систем, каждая из которых может оказаться слабым звеном с точки зрения безопасности. Риски в банковской сфере столь же высоки, сколь и разнообразны: действия злоумышленников*, технические неполадки, человеческий фактор… Этот список можно продолжать.*

Банковская безопасность – довольно сложное понятие, включающее в себя три составляющих элемента:

1) финансово–правовой, – он проявляется посредством регулирования экономических стандартов деятельности кредитных организаций, обязательных экономических нормативов и требований по поддержанию резервов (фондов)).

2) административно–правовой – включает деятельность Банков Беларуси, государственных органов, а также кредитных организаций по осуществлению управленческих функций при осуществлении банковских операций и сделок (включая обеспечение непрерывности бизнеса и корпоративное управление, в том числе – управление персоналом).

3) информационная безопасность – как совокупность технических регламентов и требований, позволяющих обеспечить защиту информации и самих банковских систем от неправомерного вмешательства и иных угроз (рисков)[1].

Основные проблемы в вопросах защиты информации на сегодняшний день — это существенные пробелы в законодательстве РБ, отсутствие национальных стандартов и системы сертификации в этой области. С ростом интереса потребителей к защите информации увеличилось количество производителей и поставщиков средств защиты, заполняющих рынок изделиями, качествен-

ные характеристики которых неизвестны и никем не гарантируются. Недостаточное количество данных о таких средств чревато непредсказуемыми последствиями как для самого Национального банка, так и для всей банковской системы страны. Считаю, что заинтересованным государственным министерствам и ведомствам следует начать работы по созданию в Республике сети сертификационных центров и испытательных лабораторий в области защиты информации.

”В сложившихся условиях Национальным банком совместно с рядом государственных организаций начаты работы по использованию Закона Республики Беларусь «Об электронных документах, используемых в банковской сфере» и комплекса отраслевых стандартов Национального банка по цифровой подписи”[2].

Проблемы защиты информации требуют сугубо профессионального похода, что в свою очередь предполагает наличие соответствующих специалистов и создание системы их регулярной подготовки. С этой целью руководством Национального банка было принято решение о создании Отдела защиты информационных систем, в компетенцию которого входят вопросы обеспечения безопасности информации в информационной системе банка и в общенациональных системах электронного перевода денежных средств. Вопросы защиты информации становятся особенно актуальными при использовании электронных данных и переводе денежных средств в реальном времени.

Итак, можно сделать вывод, что основной проблемой IT–безопасности служит отсутствие комплексной системы защиты. Часто в банке имеется лишь минимальный набор средств: межсетевой экран наряду с антивирусом и средством криптографической защиты данных. Конечно, данные элементы недостаточны для решения всего комплекса проблем, упомянутых выше. Следует применять как системы обнаружения и предотвращения атак, так и системы мониторинга событий безопасности совокупно со средствами анализа защищенности. Определенные трудности возникают в случае неправильной конфигурации используемых средств защиты.

Проблема, кроме того, кроется и в несовершенстве уголовного законодательства. Согласно законам расследование преступления происходит по месту его совершения. Но, в том случае, когда похищенные средства переводятся на разные счета в разных регионах и за рубежом, определить точное место совершения преступления невозможно. И эта правовая неопределённость весьма затрудняет расследование.

Добиться должного уровня информационной безопасности в банках, конечно же, невозможно без соответствующей работы с сотрудниками. Не случайно все чаще встречается понятие «инсайдер», подразумевающее нарушение конфиденциальности информации со стороны персонала.

Лишь решение всех вышеуказанных проблем позволит говорить о существенном повышении общего уровня информационной безопасности банков, в данном случае следует учитывать как правовые, так и технические, кадровые и организационные аспекты. Кроме того, речь идет и о более широкой интеграции службы IT в структуру управления банком: централизация, виртуализация в данном случае становятся во главе системы. В идеале каждое приложение автоматизированной банковской системы должно интегрироваться общей информационной системой и централизованно исполняться на серверах головного офиса[3].

Нельзя ни на секунду забывать, что информационная безопасность, каким бы высоким не был ее уровень – это не готовый продукт, который можно купить, внедрить и забыть. Это система, требующая непрерывной работы.

Итак, можно выделить несколько основных правил, следование которым позволит избежать утечку банковской информации и сделать работу IT–сотрудников более продуктивной:

•Непрерывный контроль за персоналом банка: прием на работу сотрудников, мотивация персонала, обучающие курсы, аттестации и т. п.;

• Наличие развитой технологической основы: специализированные технические средства, оборудование;

• Постоянный мониторинг и всесторонний контроль над аппаратно–программным комплексом;

• Обеспечение информационной безопасности: многоуровневая система защиты информации, контроль входящего трафика, DDoS–устойчивость;

• Круглосуточная техническая поддержка для обеспечения бесперебойной работы дата–центра.

Список использованных источников

1.Евразийский Юридический Портал [Электронный ресурс]. 2011. – Режим доступа: http://www.eurasialegal.info/index.php?option=com_jcontentplus&view=article&id=853:2011–06–27–09–22–46&catid=2:right–of–the–countries–cis – Дата доступа: 16.03.2014.

2. Об электронном документе и электронной цифровой подписи [Электронный ресурс].2013. – Режим доступа: http://pravo.by/main.aspx?guid=3871&p0=H10900113&p2={NRPA} –Дата доступа: 16.03.2014.

3.Интеллектуальный банк [Электронный ресурс] / Илья Глазырин. – Москва, 2012. – Режим доступа: http://www.int–bank.ru/. – Дата доступа: 22.03.2014.